

REMARKS

Applicants appreciate the thorough examination of the present application as evidenced by the Office Action. Applicants submit that the present rejections should be withdrawn for at least the reasons discussed below.

Interview Summary:

Applicants note that the Interview Summary provided by the Examiner with the August 8, 2005 copy of the Office Action reflects the entirety of the matters discussed during the interview. Applicants appreciate the courtesy of the Examiner during the interview and the re-issuance of the Office Action and re-setting of the due date for Applicants' response to run from August 8, 2005.

The Prior Art Rejections:

Claims 1-51 stand rejected under 35 U.S.C. § 102(e) as anticipated by United States Patent No. 6,735,701 to Jacobson ("Jacobson"). Office Action, p. 2. Applicants submit that the claims are patentable over Jacobson for at least the reasons discussed below.

Independent Claim 1 is Patentable Over Jacobson:

Independent Claim 1 has been amended above to recite a security policy document "in a portable representation language" and that the security policy document includes "a plurality of data elements for communicating the security policy" to the users and "at least one data element for implementing the securing policy on computer systems in the network." Support for these amendments can be found, for example, at paragraph 40 (page 15, corresponding to paragraph 53 in the published application), paragraph 44 (page 16) and paragraph 47 (page 17) of the present specification. Applicants can find no disclosure of any of these recitations in Jacobson.

With respect to the portable representation language recitation, Claim 15 as filed recites a "markup language," which is a portable representation language. In rejecting

Claim 15, the Office Action cites to the following text in Jacobson:

The program steps implementing this invention are stored in the memory and executed by the computer processor. The present invention is may be implemented using an intranet based application that can be stored on central servers, waiting to be called up and manipulated via a Web browser from any location.

Jacobson, Col. 5, lines 2-7. Office Action, p. 4. To the extent this section is relevant at all, it may be in the reference to "an intranet based application" that may be "called up and manipulated via a Web browser." As such, an HTML type provision of information to remote locations executing a browser is inferred. However, it does not follow that the HTML would disclose or suggest the "security policy document" of Claim 1, instead, it merely indicates that screen display information, that may include information related to a "policy" may be provided to remote locations in an HTML form. The "policy training module" and other modules of Jacobson are not described as creating a specific "security policy **document**" that contains such HTML form information. Instead, such displays may be standard page or frame displays saved on a system, text information stored in a database or the like and extracted by the policy training module and/or various known other ways to create HTML pages and the like.

Furthermore, the Office Action appears to not even distinguish between the recited policy management **program** and the recited policy **document** of Claim 1 in applying Jacobson. The "network security policies stored in the database" of Jacobson, while arguably a document, are not even alleged in the Office Action as disclosing the particulars of "a security policy document" as recited in Claim 1 nor does Jacobson appear to discuss "enabling creation" of such stored policies by the described policy compliance monitor 110 or effectiveness module 120 shown as coupled to the policy repository 125 of Figure 1 of Jacobson.

Accordingly, Jacobson clearly does not anticipate Claim 1 for at least these reasons. Should the rejection be maintained, Applicants request a clarification of what in Jacobson is alleged as teaching the policy management program, the security policy document and the portable representation language recitations of Claim 1.

Furthermore, as amended, Claim 1 further recites that the security policy document include both a plurality of data elements for communicating to users and at least one data element for implementing the security policy. Thus, the recited "security policy **document**" includes data elements, which also appear not to be discussed in Jacobson. In addition, the data elements must include at least one data element that is used for implementing the security policy on computer systems, as contrasted with communicating the policy to users. Applicants note that as filed Claim 11 recites technical controls "for implementing the security policy on at least one first computer." In rejecting Claim 11, the Office Action asserts that these recitations are disclosed by the following text in Jacobson:

To overcome the limitations in the prior art described above, and to overcome other limitations that will become apparent upon reading and understanding the present specification, the present invention discloses a method and apparatus for maintaining policy compliance on a computer network. A system in accordance with the principles of the invention performs the steps of electronically monitoring network user compliance with a network security policy stored in a database, electronically evaluating network security policy compliance based on network user compliance, and **electronically undertaking a network policy compliance action in response to network security policy compliance. The network policy compliance actions may include electronically implementing a different network security policy selected from network security policies stored in the database**, generating policy effectiveness reports, and providing a retraining module to network users.

Jacobson, Col. 2, lines 3-18 (emphasis added);

The Policy Compliance Monitor 110 works with the Policy Effectiveness Module 120 to provide network user compliance monitoring with network security policy stored in a database, it electronically evaluates network security policy compliance based on network user compliance, and **undertakes a network policy compliance action in response to network security policy compliance**. Network user compliance monitoring is defined as monitoring network activity to insure users are in compliance with the organization's network security policies. Network security policy is a set of rules designed to limit an organization's risk and liability.

FIG. 5 is a block diagram further illustrating the operation of the policy effectiveness system according to an embodiment of this invention.

In re: Lineman et al.
Serial No. 09/966,006
Filed: September 28, 2001
Page 14 of 19

Jacobson, Col. 10, line 57 to Col. 11, lines 3 (emphasis added); and

Block 202 represents the policy training module 105 *presenting the network user with screen personality options*. A screen personality represents a person who is executing the training session under an assumed screen name and identity. In other words, a screen relates to a real person taking a training session. The user is typically *presented with a screen and is asked to choose a screen name and identity (e.g., Avatar) from a list of screen personalities for the training session*. Such screen personalities give users greater privacy and the freedom to answer policy questions without fear of retaliation from other employees participating in the program.

Jacobson, Col. 6, lines 47-57 (emphasis added).

Applicants have attempted to highlight in bold in the above sections anything even remotely related to "implementing the security policy on the computer systems. At most these statements refer to "compliance actions" that may include "implementing a different security policy." As such, the term "implementing" is found as well as "security policy." However, as stated in the underlined portion of Jacobson above, a "security policy" is identified as "a set of rules designed to limit an organization's risk and liability." Implementing is described in Jacobson as training users on policy and, more particularly, using that training as a way to develop policies. See, Jacobson, Col. 5, lines 36-50. Thus, Applicants' submit that the portions of Jacobson relied on in rejecting Claim 1 (and Claim 11), while they recite "implementing a different security policy," do not disclose or even suggest creation of a security policy **document** including at least one **data element** for implementing the security policy on **computer systems**. Instead, they, at most, suggest changing rules for **users** and training **users** on those new rules to encourage compliance by increased user appreciation of the "organization's risk and liability." Accordingly, the rejection of Claim 1 should also be withdrawn for at least these additional reasons.

Independent Claim 11 is Patentable Over Jacobson:

Independent Claim 11, as discussed above with reference to Claim 1, includes recitations related to a security policy **document** and technical controls "for implementing the security policy on at least one first computer." Accordingly, the

rejection of Claim 11 as anticipated by Jacobson should be withdrawn at least for reasons substantially similar to those discussed with reference to the corresponding recitations of Claim 1 above.

In addition, Claim 11 also includes the recitation of "enabling creation of a security policy document ... by enabling selection of security policies from a set of options." The Office Action asserts that these recitations are taught by the same sections of Jacobson as reproduced above. In reviewing these sections with reference to these recitations, Applicants assume that the Office Action is relying on the italicized portions in the excerpts above related to selection of a screen personality from presented "screen personality option." However, these "options" have nothing to do with security policies as recited in Claim 11. As stated by Jacobson, the "screen personalities give users greater privacy and the freedom to answer policy questions without fear of retaliation from other employees participating in the program." Jacobson, Col. 6, lines 55-58. Accordingly, the anticipation rejection of Claim 11 should also be withdrawn for at least these additional reasons.

Independent Claim 26 is Patentable Over Jacobson:

Independent Claim 26, like Claim 1, recites a distinct program and "security policy document." Accordingly, the rejection of Claim 26 should be withdrawn at least based on substantially similar reasons to those discussed above with reference to the corresponding recitations of Claim 1.

Claim 26 also recites configuring the security policy document to create both "a human-readable security policy document" and a "machine-readable security policy document containing technical controls readable by" a computer. In rejecting Claim 26, the Office Action relies on the same excerpts of Jacobson as reproduced above that were used in rejecting Claims 1 and 11. Applicants assume this rejection also relies on the portions highlighted in bold in the excerpts above as disclosing the machine-readable technical controls in a security policy document. However, for reasons similar to those discussed with reference to Claim 1, Applicants submit that the cited experts of

In re: Lineman et al.
Serial No. 09/966,006
Filed: September 28, 2001
Page 16 of 19

Jacobson do not include an anticipatory disclosure of such particular recitations of inclusion of human and machine information in a security policy document to provide security policy management "for one or more **users and one or more first computers** in a network" as recited in Claim 1 (emphasis added). Accordingly, the anticipation rejection of Claim 26 should also be withdrawn for at least these additional reasons. Should the rejection of Claim 26 be maintained, Applicants request a clarification of the basis for asserting that these recitations are found in Jacobson.

Independent Claim 51 is Patentable Over Jacobson:

Independent Claim 51, like Claim 1, recites a security policy document and separate program. In addition, Claim 51 includes human-readable and machine-readable format recitations similar to Claim 26. Accordingly, the rejection of Claim 51 should be withdrawn at least based on substantially similar reasons to those discussed above with reference to the corresponding recitations of Claims 1 and 26.

Claim 51 also includes recitations related to a second program for monitoring security compliance and a third program "for receiving the machine-readable format of the security policy document." The rejection of Claim 51 relies on the same excerpts from Jacobson as reproduced above. Applicants submit the rejection of Claim 51 should also be withdrawn at least as these recitations appear not to be disclosed in these excerpts from Jacobson. With respect to these additional recitations of Claim 51, Applicants are unable to determine what is relied on in the Office Action as disclosing the respective second and third programs and the recitations related thereto. Accordingly, if the rejection of Claim 51 is not withdrawn, Applicants request clarification of the basis for this rejection.

The Dependent Claims Are Patentable Over Jacobson:

The dependent claims are patentable at least based on their dependence from a patentable independent claim. In addition, some of the dependent claims are separately patentable. For example, Claim 5 includes recitations related to selection of security policies from "a set of options." Accordingly, Claim 5 is separately patentable for

substantially similar reasons as those discussed above with reference to the corresponding recitations of independent Claim 11.

Claim 13 recites that the computer systems "operate in accordance with different operating systems." The Office Action asserts that these recitations are disclosed by the following portions of Jacobson:

There is a further need for network communications software programs that offers robust policy compliance assistance, policy effectiveness monitoring and reporting.

Jacobson, Col. 1, lines 60-63; and

The program steps implementing this invention are stored in the memory and executed by the computer processor. The present invention is may be implemented using an intranet based application that can be stored on central servers, waiting to be called up and manipulated via a Web browser from any location. Those skilled in the art will recognize that

Jacobson, Col. 2, lines 5-7. Applicants can find no discussion of operating systems, nonetheless different operating systems, in either of these excerpts. Accordingly, Claim 13 is separately patentable for at least these reasons. Claims 14, 47, 15, 48, 20, 40 and 38 are similarly rejected based on one or both of these excerpts of Jacobson and Applicants are, likewise, unable to find any basis in these excerpts for the rejections of these claims. These claims are separately patentable for at least these additional reasons.

Claim 16 recites "distributing detect rules" to at least one first computer. The rejection of Claim 16 at page 5 of the Office Action is based on the following excerpt from Jacobson:

performed by the policy training module 105 in performing the generating a network security policy step represented by block 220 according to an embodiment of this invention;

Jacobson, Col. 8, lines 7-10. Applicants submit that there is no discussion related to distributing detect rules in this excerpt and Claim 16 is separately patentable for at least these additional reasons.

Claims 18 and 19 include recitations related to distributing and converting technical controls. The rejections of Claims 18 and 19 at page 5 of the Office Action are

In re: Lineman et al.
Serial No. 09/966,006
Filed: September 28, 2001
Page 18 of 19

based on the following excerpt from Jacobson:

The network policy compliance actions may include electronically implementing a different network security policy selected from network security policies stored in the database, generating policy effectiveness reports, and providing a retraining module to network users.

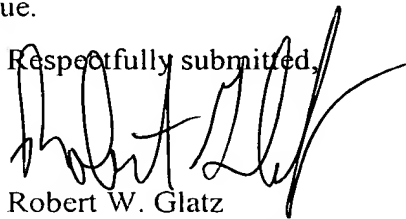
Jacobson, Col. 2, lines 14-19. Applicants submit that implementing a different security policy does not disclose distributing or converting technical controls or even, as discussed above, teach technical controls. Accordingly, Claims 18 and 19 are separately patentable for at least these additional reasons.

The newly added dependent Claims 53-56 include various recitations related to particular data elements and platform control elements for different operating system platforms. Such embodiments are described, for example, in paragraphs 43-48 (pages 16-17) of the present application. Applicants submit that the recitations of these claims are also not disclosed by Jacobson. Accordingly, Claim 53-56 are separately patentable for at least these additional reasons.

CONCLUSION

Applicants respectfully submit that, for the reasons discussed above, the references cited in the present rejections do not disclose or suggest the present invention as claimed. Accordingly, Applicants respectfully request allowance of all the pending claims and passing this application to issue.

Respectfully submitted,



Robert W. Glatz
Registration No. 36,811

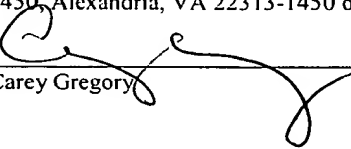
Myers Bigel Sibley & Sajovec
P.O. Box 37428
Raleigh, NC 27627
(919) 854-1400 phone
(919) 854-1401 fax

In re: Lineman et al.
Serial No. 09/966,006
Filed: September 28, 2001
Page 19 of 19



Certificate of Mailing under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on September 19, 2005.



Carey Gregory

450401